IN THE CLAIMS

Claims 1, 5, 9-10, 18, and 21-22 are amended; claims 6-8, 14-17, 19-20, and 24 are cancelled without prejudice; and claim 4 previously has been cancelled without prejudice:

1. (CURRENTLY AMENDED) An apparatus for encrypting/decrypting a real-time input stream, comprising:

a control unit receiving a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream into data blocks, providing the data blocks for encryption or decryption, receiving encrypted or decrypted data blocks, converting the received encrypted or decrypted data blocks into bytes, and outputting the bytes;

a key schedule unit ~~carrying out~~ providing a round key ~~schedule~~ for every round in accordance with an input key having a variable ~~key~~ size ~~so as~~ to ~~output a key~~ provide the round key for the encryption or decryption for each round, wherein the ~~variable~~ input key size is one of 128, 192, and 256 bits; and

a block round unit receiving the converted data blocks from the control unit, receiving the round key from the key schedule unit, encrypting or decrypting the received data blocks, and providing the encrypted or decrypted data blocks to the control unit,

wherein the key schedule unit selects a 128 bit round key to the block round unit for each round using a key register having a capacity of {(size of an inputted block) * (size of one round)}.

~~wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit.~~

2. (PREVIOUSLY PRESENTED) The apparatus of claim 1, the control unit comprising:

an input buffer storing the data stream of bytes and converting the received data stream into the data blocks having a predetermined size so as to output the converted data blocks to the block round unit; and

an output buffer receiving the data blocks encrypted or decrypted in the block round unit and converting the received data blocks into the byte units so as to output a converted data.

3. (PREVIOUSLY PRESENTED) The apparatus of claim 2, wherein the block round unit completes all round calculation of data having been currently encrypted or decrypted before a next data block is inputted from the control unit and then stores the corresponding result in the output buffer of the control unit.

4. (CANCELLED)

5. (CURRENTLY AMENDED) The apparatus of ~~claim 5~~ claim 1, the key schedule unit comprising:

a key expansion unit expanding the inputted key value into a size amounting to {block size * (count of rounds +1)}; and

a key selection unit selecting ~~a 128~~ the 128 bit key required for each round from the expanded key value ~~so as to output~~ to provide the selected key to the block round unit.

6. (CANCELLED)

7. (CANCELLED)

8. (CANCELLED)

9. (CURRENTLY AMENDED) The apparatus of claim 1, wherein the control unit generates a control signal to produce the ~~key value~~ selected 128 bit round key every round and then outputs the control signal to the key schedule unit.

10. (CURRENTLY AMENDED) An apparatus for encrypting/decrypting a real-time input data stream wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, comprising:

a control unit receiving a data stream in first data format, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and ~~carrying out~~ providing a round key ~~schedule~~ for every round in response to an input key having a variable ~~key~~ size ~~and outputting a key value~~ for the encryption or decryption for each round wherein the ~~variable~~ input key size is one of 128, 192, and 256 bits; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the round key from the key schedule unit ~~so as to carry out at least one of the~~ for encryption or decryption of each round, and ~~outputting~~ providing the encrypted or decrypted result to the control unit,

~~wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit~~

wherein the key schedule unit expands the input key into a size of {second data format size * (count of rounds +1)}, selects an N bit key required for each round from the expanded key value, and provides the selected N bit key to the block round unit for each round, and

wherein the key schedule unit comprises a key register having a capacity of {(size of an inputted block) * (size of one round)}.

11. (PREVIOUSLY PRESENTED) The apparatus of claim 10, wherein the first data format is in bytes, and the second data format is a data block.

12. (ORIGINAL) The apparatus of claim 10, the control unit comprising:

an input buffer storing the data stream of the first data format and converting the received data stream into the data of the second data format having a predetermined size; and

an output buffer receiving data in the second data format and converting the data into the first data format.

13. (ORIGINAL) The apparatus of claim 12, wherein the block round unit substantially completes all data encryption or decryption processing before a next set of data is inputted from the control unit and stores the corresponding result in the output buffer of the control unit.

14. (CANCELLED)

15. (CANCELLED)

16. (CANCELLED)

17. (CANCELLED)

18. (CURRENTLY AMENDED) The apparatus of ~~claim 17~~ claim 10, wherein the N bit key is equal to a 128 bit key.

19. (CANCELLED)

20. (CANCELLED)

21. (CURRENTLY AMENDED) The apparatus of claim 10, wherein the control unit generates a control signal to produce the round key ~~value~~ in every round.

22. (CURRENTLY AMENDED) A real-time encryption/decryption apparatus, comprising:

a control unit receiving a data stream in first data format wherein the data stream data is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and ~~carrying out~~ providing a round key ~~schedule~~ in a predetermined period in response to an input key having a variable ~~key~~ size, wherein the ~~variable~~ input key size is one of 128, 192, and 256 bits, and wherein the key schedule unit has a key register capable of processing the input key required ~~substantially~~ for the predetermined period; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the round key ~~value~~ from the key schedule unit ~~so as to carry out at least one of the~~ for encryption or decryption of each round,

wherein a size of the key register is no less than {(second data format size) * (size of one period)}

~~wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit~~.

23. (PREVIOUSLY PRESENTED) The apparatus of claim 22, wherein the first data format is in bytes, and the second data format is in a data block.

24. (CANCELLED)

25. (PREVIOUSLY PRESENTED) A method of controlling a data protection key, the method comprising:

generating a data key according to a start key signal, the data key generated according to at least one of a predetermined period and a scheduled period, wherein the scheduled period depends on a change of the data key size;

checking validity of the data key; and

encrypting data corresponding to the period with the data key,

wherein the start key signal is transmitted for generating the data key.

26. (PREVIOUSLY PRESENTED) The method of claim 25, further comprising a data key valid signal provided with the data key for encryption and decryption.

27. (PREVIOUSLY PRESENTED) The method of claim 25, wherein the data are encrypted according to the start key signal in real time.